

109TH CONGRESS
1ST SESSION

H. R. 3140

To expand the protections for sensitive personal information in Federal law to cover the information collection and sharing practices of unregulated information brokers, to enhance information security requirements for consumer reporting agencies and information brokers, and to require consumer reporting agencies, financial institutions, and other entities to notify consumers of data security breaches involving sensitive consumer information, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JUNE 30, 2005

Ms. BEAN (for herself, Mr. DAVIS of Alabama, Mr. FRANK of Massachusetts, Mrs. MALONEY, Mr. GUTIERREZ, Mr. WATT, Mr. ACKERMAN, Mr. FORD, Mr. CROWLEY, Mr. CLAY, Mrs. MCCARTHY, Mr. LYNCH, Ms. WASSERMAN SCHULTZ, and Ms. MOORE of Wisconsin) introduced the following bill; which was referred to the Committee on Financial Services

A BILL

To expand the protections for sensitive personal information in Federal law to cover the information collection and sharing practices of unregulated information brokers, to enhance information security requirements for consumer reporting agencies and information brokers, and to require consumer reporting agencies, financial institutions, and other entities to notify consumers of data security breaches involving sensitive consumer information, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Consumer Data Secu-
5 rity and Notification Act of 2005”.

6 **SEC. 2. AMENDMENTS TO THE FAIR CREDIT REPORTING**
7 **ACT.**

8 (a) FCRA COVERAGE OF DATA BROKERS.—Section
9 603(d) of the Fair Credit Reporting Act (15 U.S.C.
10 1681a(d)) is amended by adding at the end the following
11 new paragraph:

12 “(4) COMMUNICATION OF PERSONALLY IDENTIFI-
13 FIABLE INFORMATION BY CERTAIN PERSONS IN-
14 CLUDED.—The term ‘consumer report’ shall also in-
15 clude any written, oral, electronic, or other commu-
16 nication of any information by any person which, for
17 monetary fees, dues or other compensation, regularly
18 engages in whole or in part in the practice of assem-
19 bling or evaluating personally identifiable informa-
20 tion for the purpose of furnishing reports to third
21 parties that includes the name of any consumer and
22 any of the following information relating to such
23 consumer:

24 “(A) Any Social Security account number.

25 “(B) Any driver’s license number.

1 “(C) Any other identification number
2 issued by a State or the Federal Government.

3 “(D) Any bank, savings association, credit
4 union, or investment account number.

5 “(E) Any credit card, or debit card ac-
6 count number.

7 “(F) Any password, access code, or secu-
8 rity code relating to a bank, savings association,
9 credit union, or investment account number or
10 credit or debit card account number.”.

11 (b) VERIFICATION STANDARDS FOR USERS OF CON-
12 SUMER REPORTS.—Section 604(f) of the Fair Credit Re-
13 porting Act (15 U.S.C. 1681b(f)) is amended—

14 (1) by striking “and” at the end of paragraph
15 (1);

16 (2) by redesignating paragraph (2) as para-
17 graph (3); and

18 (3) by inserting after paragraph (1) the fol-
19 lowing new paragraph:

20 “(2) the identity of the person requesting the
21 consumer report has been verified, pursuant to sec-
22 tion 607(a), in accordance with procedures which the
23 Commission shall prescribe in regulation; and”.

24 (c) DATA SECURITY STANDARDS AND NOTIFICATION
25 OF SECURITY BREACHES.—

1 (1) IN GENERAL.—The Fair Credit Reporting
2 Act (15 U.S.C. 1681 et seq.) is amended by adding
3 at the end the following new section:

4 **“SEC. 630. PROTECTION OF NONPUBLIC CONSUMER INFOR-**
5 **MATION.**

6 “(a) IN GENERAL.—Notwithstanding any other pro-
7 vision of this title, each consumer reporting agency shall
8 have an affirmative and continuing obligation to respect
9 the privacy of consumers and to protect the security and
10 confidentiality of consumers nonpublic personal informa-
11 tion.

12 “(b) SAFEGUARDS REQUIRED.—In furtherance of
13 subsection (a), the Commission shall establish appropriate
14 standards, by regulation, for consumer reporting agencies
15 relating to administrative, technical, and physical safe-
16 guards—

17 “(1) to insure the security and confidentiality of
18 consumer records and information;

19 “(2) to protect against any anticipated threats
20 or hazards to the security of such records; and

21 “(3) to protect against unauthorized access to
22 or use of such records or information which could
23 result in substantial harm or inconvenience to any
24 customer.

1 “(c) NOTIFICATION OF DATA SECURITY
2 BREACHES.—

3 “(1) IN GENERAL.—The regulations prescribed
4 under subsection (b) shall include requirements for
5 the notification of consumers following the discovery
6 of a breach of security of any data system main-
7 tained by the consumer reporting agency in which
8 sensitive consumer information was, or is reasonably
9 believed to have been, acquired by an unauthorized
10 person.

11 “(2) CONTENT OF REGULATIONS.—The regula-
12 tions prescribed under paragraph (1) shall include
13 the following requirements or provisions:

14 “(A) A requirement that a consumer re-
15 porting agency provide written notice to a con-
16 sumer whenever such agency becomes aware
17 that sensitive personal information relating to
18 the consumer has been, or is reasonably be-
19 lieved to have been, acquired by an unauthor-
20 ized person, unless the consumer reporting
21 agency, after appropriate investigation—

22 “(i) reasonably concludes that misuse
23 of the information is unlikely to occur;

1 “(ii) notifies the appropriate law en-
2 forcement agency of the data security
3 breach; and

4 “(iii) takes appropriate steps to rem-
5 edy the security breach and safeguard the
6 interests of affected consumers.

7 “(B) A requirement that the notices re-
8 quired under paragraph (1) be provided by a
9 consumer reporting agency without unreason-
10 able delay following—

11 “(i) the discovery by such agency of a
12 breach of security in the data system; and

13 “(ii) reasonable actions which the con-
14 sumer reporting agency shall take to inves-
15 tigate the nature and intent of the breach,
16 prevent further unauthorized access or dis-
17 closure, and restore the reasonable integ-
18 rity of the data system.

19 “(C) A provision that allows for reasonable
20 delay of such notification to the consumer
21 under paragraph (1) upon the written request
22 of a law enforcement agency which has deter-
23 mined that the notification required under
24 paragraph (1) would seriously impede a crimi-
25 nal investigation.

1 “(D) A provision that the written notice
2 required under paragraph (1) may be made by
3 an electronic transmission only if—

4 “(i) the consumer has provided prior
5 consent to receive any such notice by elec-
6 tronic transmission; and

7 “(ii) the notice is consistent with the
8 provisions permitting electronic trans-
9 mission of notices under section 101 of the
10 Electronic Signatures in Global and Na-
11 tional Commerce Act.

12 “(E) A requirement that the notification
13 provided to consumers include—

14 “(i) the date on which the consumers
15 nonpublic personal information was, or is
16 reasonably believed to have been, acquired
17 by an unauthorized person;

18 “(ii) the specific information that was,
19 or is reasonably believed to have been, ac-
20 quired by an unauthorized person, includ-
21 ing Social Security account numbers, bank
22 or investment account numbers, credit or
23 debit card account numbers, or any pass-
24 word or code relating to such accounts;

1 “(iii) the actions taken by the con-
2 sumer reporting agency to address or rem-
3 edy the security breach and prevent unau-
4 thorized use of nonpublic personal informa-
5 tion;

6 “(iv) the summary of rights of con-
7 sumer victims of fraud or identity theft
8 prepared by the Federal Trade Commis-
9 sion under section 609(d) and information
10 on how to contact the Commission for
11 more detailed information; and

12 “(v) the toll-free telephone number
13 where consumers may obtain additional in-
14 formation about the security breach and an
15 explanation of available options to protect
16 their consumer file from unauthorized ac-
17 cess.

18 “(3) TREATMENT OF ENCRYPTED INFORMA-
19 TION.—For purposes of the regulations prescribed
20 under paragraph (1), the Commission shall—

21 “(A) permit a consumer reporting agency,
22 in connection with any determination pursuant
23 to paragraph (2)(A)(i), to reasonably conclude
24 that misuse of information is unlikely to occur
25 where the sensitive consumer information ac-

quired, or believed to have been acquired, by an unauthorized person consists of information that has been encrypted in a manner consistent with standards set forth under subparagraph (B);

“(B) identify appropriate standards for encryption of personal and financial information for purposes of subparagraph (A), taking into consideration the Advanced Encryption Standard adopted by the National Institute of Standards and Technology for use by the Federal Government; and

“(C) establish appropriate criteria for determining whether information that has been encrypted has been accessed by an unauthorized person, and whether misuse of such information is likely to occur and notification is required pursuant to this section.”.

(2) CLERICAL AMENDMENT.—The table of contents for the Fair Credit Reporting Act is amended by inserting after the item relating to section 129 the following new item:

“630. Protection of nonpublic consumer information.”.

(d) USE OF CONSUMER REPORTS FOR PRIVATE INVESTIGATIONS.—

1 (1) IN GENERAL.—Section 604(a)(3) of the
2 Fair Credit Reporting Act (15 U.S.C.1681b(a)(3)) is
3 amended—

4 (A) by striking “or” at the end of subpara-
5 graph (E);

6 (B) by redesignating subparagraph (F) as
7 subparagraph (G); and

8 (C) by inserting after subparagraph (E)
9 the following new paragraph:.

10 “(F) is a duly licensed private investigator
11 who intends to use the consumer report only in
12 connection with a lawful investigation within
13 the scope of the investigator’s license and for no
14 other purpose; or”.

15 (2) TECHNICAL AND CONFORMING AMEND-
16 MENT.—Section 603(k)(1)(B)(iv)(I) of the Fair
17 Credit Reporting Act (15 U.S.C.
18 1681a(k)(1)(B)(iv)(I)) is amended by striking
19 “604(a)(3)(F)(ii)” and inserting “604(a)(3)(G)(ii)”.

20 (e) REGULATIONS.—The Federal Trade Commission
21 shall prescribe such regulations as the Commission deter-
22 mines to be necessary to implement the amendments made
23 by this section and such regulations shall be published in
24 final form before the end of the 6-month period beginning
25 on the date of the enactment of this Act.

1 **SEC. 3. AMENDMENTS TO TITLE V OF THE GRAMM-LEACH-**
2 **BLILEY ACT.**

3 (a) NOTIFICATION OF SECURITY BREACHES.—Sec-
4 tion 501 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801)
5 is amended by adding at the end the following new sub-
6 section:

7 “(c) NOTIFICATION OF DATA SECURITY
8 BREACHES.—

9 “(1) IN GENERAL.—In establishing standards
10 pursuant to subsection (b), each agency or authority
11 described in section 505(a) shall require, in regula-
12 tion, that a financial institution notify customers fol-
13 lowing the discovery of a breach of security of any
14 data system maintained by the financial institution
15 in which nonpublic personal information was, or is
16 reasonably believed to have been, acquired by an un-
17 authorized person.

18 “(2) CONTENT OF REGULATIONS.—The regula-
19 tions prescribed under paragraph (1) shall include
20 the following requirements or provisions:

21 “(A) A requirement that a financial insti-
22 tution provide written notice to a customer
23 whenever the institution becomes aware that
24 sensitive personal information relating to the
25 customer has been, or is reasonably believed to
26 have been, acquired by an unauthorized person,

1 unless the financial institution, after appro-
2 priate investigation, reasonably concludes that
3 misuse of the information is unlikely to occur,
4 and—

5 “(i) promptly notifies its primary Fed-
6 eral financial regulatory agency of the data
7 security breach;

8 “(ii) notifies the appropriate law en-
9 forcement agency of the data security
10 breach; and

11 “(iii) takes appropriate steps to rem-
12 edy the security breach and safeguard the
13 interests of affected customers, including
14 monitoring the affected customers accounts
15 for unusual or suspicious activity.

16 “(B) A requirement that the notice re-
17 quired under paragraph (1) be provided by a fi-
18 nancial institution without unreasonable delay
19 following—

20 “(i) the discovery by the financial in-
21 stitution of a breach of security in the data
22 system;

23 “(ii) reasonable investigation of the
24 nature and scope of the security breach,
25 including identification of the customer in-

1 formation systems and specific customer
2 information or accounts that may have
3 been accessed;

4 “(iii) notification of the primary Fed-
5 eral financial regulatory agency for the fi-
6 nancial institution;

7 “(iv) notification of appropriate law
8 enforcement agencies; and

9 “(v) reasonable measures to prevent
10 further unauthorized access or disclosure
11 and to restore the reasonable integrity of
12 the data system.

13 “(C) A provision establishing minimum
14 standards for investigations of the nature and
15 scope of security breaches, including any limita-
16 tion on the duration of such investigations that
17 the agency or authority may consider appro-
18 priate to prevent substantial harm or inconven-
19 ience to any customer;

20 “(D) A provision that allows for reasonable
21 delay of such notification upon the written re-
22 quest of a law enforcement agency which has
23 determined that the notification required under
24 paragraph (1) would seriously impede a crimi-
25 nal investigation;

1 “(E) A provision that the written notice
2 required under paragraph (1) may be made by
3 an electronic transmission only if—

4 “(i) the customer has provided prior
5 consent to receive any such notice by elec-
6 tronic transmission; and

7 “(ii) the notice is consistent with the
8 provisions permitting electronic trans-
9 mission of notices under section 101 of the
10 Electronic Signatures in Global and Na-
11 tional Commerce Act.

12 “(F) A requirement that the notification
13 provided to consumers include—

14 “(i) the date on which the customers
15 nonpublic personal information was, or is
16 reasonably believed to have been, acquired
17 by an unauthorized person;

18 “(ii) the specific information that was,
19 or is reasonably believed to have been, ac-
20 quired by an unauthorized person, includ-
21 ing Social Security account numbers, bank
22 or investment account numbers, credit or
23 debit card account numbers, or any pass-
24 word or code relating to such accounts;

1 “(iii) the actions taken by the finan-
2 cial institution to address or remedy the
3 security breach and prevent unauthorized
4 use of nonpublic customer information;

5 “(iv) the summary of rights of con-
6 sumer victims of fraud or identity theft
7 prepared by the Federal Trade Commis-
8 sion under section 609(d) of the Fair
9 Credit Reporting Act and information on
10 how to contact the Commission for more
11 detailed information; and

12 “(v) the toll-free telephone number
13 where customers may obtain additional in-
14 formation about the security breach and
15 explanations of available options to protect
16 their consumer file from unauthorized ac-
17 cess.

18 “(G) A requirement concerning any other
19 action or disclosure that the agency or author-
20 ity determines necessary or appropriate to carry
21 out the intent of this subsection.

22 “(3) CERTAIN PERSONS TREATED AS FINAN-
23 CIAL INSTITUTIONS FOR THIS SUBSECTION.—

24 “(A) IN GENERAL.—For purposes of this
25 subsection (and sections 504, 505, and 507 to

1 the extent applicable with respect to this sub-
2 section), the term ‘financial institution’ includes
3 any person or organization that, in the regular
4 course of business, collects and maintains writ-
5 ten or electronic files containing individually
6 identifiable information on customer trans-
7 actions, including any bank, savings association,
8 or credit union account number, credit card or
9 debt card number, and any other payment ac-
10 count number, or any password, access code, or
11 security code pertaining to any such account or
12 any credit card or debit card.

13 “(B) NOTIFICATION.—A person or organi-
14 zation described in subparagraph (A) that is re-
15 quired to provide written notice pursuant to
16 regulations prescribed under paragraph (1),
17 shall, promptly notify the appropriate law en-
18 forcement agency of the data security breach,
19 and provide notification, as appropriate—

20 “(i) to the customer whose payment
21 account information has been, or is reason-
22 ably believed to have been, acquired by an
23 unauthorized person, and such notification
24 includes all applicable disclosures required
25 by paragraph (2)(F);

1 “(ii) to the financial institution which
2 is the holder of the customer’s bank, sav-
3 ings association, or credit union account,
4 credit card or debit card account, or other
5 payment account which has been, or is rea-
6 sonably believed to have been, acquired by
7 an unauthorized person, which shall be in
8 such form and include such information as
9 required by regulation; or

10 “(iii) to the financial intermediary or
11 network used to effect the credit trans-
12 action, electronic fund transfer, or other
13 form of payment on behalf of the customer
14 whose payment account information has
15 been, or is reasonably believed to have
16 been, acquired by an unauthorized person,
17 which shall include the information re-
18 quired by subparagraph (C) and such
19 other information as required by regula-
20 tion.

21 “(C) RESPONSE OF FINANCIAL INTER-
22 MEDIARY OR NETWORK UPON RECEIVING NO-
23 TICE.— A financial intermediary or network
24 that receives notice of a data security breach
25 pursuant to subparagraph (B)(iii) shall prompt-

1 ly communicate to the financial institution
2 which is the holder of the bank, savings associa-
3 tion, or credit union account, credit card or
4 debit card account, or other payment account
5 with respect to which such breach occurred, all
6 necessary information pertaining to the data se-
7 curity breach, which shall include the date on
8 which the breach is reasonably believed to have
9 occurred and the name and location of the per-
10 son or organization responsible for maintaining
11 the data system where the security breach oc-
12 curred.

13 “(D) RESPONSE OF FINANCIAL INSTITU-
14 TION THAT HOLDS CUSTOMER’S ACCOUNT UPON
15 RECEIVING NOTICE.—A financial institution
16 that receives notice of a data security breach
17 pursuant to subparagraphs (B)(ii) or (C) may
18 communicate to any customer whose bank, sav-
19 ings association, or credit union account, credit
20 card or debit card account, or other payment
21 account is identified as having been, or is rea-
22 sonably believed to have been, acquired by an
23 unauthorized person, any information it receives
24 relating to the security breach, including the
25 date on which the breach is reasonably believed

1 to have occurred and the name and location of
2 the person or organization responsible for main-
3 taining the data system where the security
4 breach occurred.

5 “(E) FINANCIAL INTERMEDIARY OR NET-
6 WORK DEFINED.—For purposes of this para-
7 graph, the term ‘financial intermediary or net-
8 work’ means a credit card association, elec-
9 tronic fund transfer network, or other system,
10 clearinghouse, or network utilized by any cred-
11 itor, credit card issuer, financial institution, or
12 money transmitting business, to effect a credit
13 transaction, electronic fund transfer, or other
14 money transmitting, check clearing, or payment
15 service.

16 “(4) TREATMENT OF ENCRYPTED INFORMA-
17 TION.—The regulations prescribed under paragraph
18 (1) shall—

19 “(A) permit a financial institution, in con-
20 nection with any determination pursuant to
21 paragraph (2)(A), to reasonably conclude that
22 misuse of information is unlikely to occur where
23 the sensitive consumer information acquired, or
24 believed to have been acquired, by an unauthor-
25 ized person consists of information that has

1 been encrypted in a manner consistent with
2 standards set forth under subparagraph (B);

3 “(B) identify appropriate standards for
4 encryption of personal and financial information
5 for purposes of subparagraph (A), taking into
6 consideration the Advanced Encryption Stand-
7 ard adopted by the National Institute of Stand-
8 ards and Technology for use by the Federal
9 Government; and

10 “(C) establish appropriate criteria for de-
11 termining whether information that has been
12 encrypted has been accessed by an unauthorized
13 person, and whether misuse of such information
14 is likely to occur and notification is required
15 pursuant to this section.”.

16 (b) REGULATIONS.—The agencies and authorities de-
17 scribed in section 505(a) of the Gramm-Leach-Bliley Act
18 shall, in the manner prescribed in section 504 of such Act,
19 prescribe such regulations as the agencies and authorities
20 determine to be necessary to implement the amendments
21 made by this section and such regulations shall be pub-
22 lished in final form before the end of the 6-month period
23 beginning on the date of the enactment of this Act.

○